

PENETRATION TESTING

Identify and address your infrastructure vulnerabilities



Ransomware attacks are one of the biggest cyber threats faced by mid-market organisations. One of the best ways to help defend against ransomware is to use an expert penetration testing service to identify and address infrastructure vulnerabilities before they are exploited.

Six Degrees' Penetration Testing services give you the information you need to enhance your protection against ransomware and other cyber-attacks. All of our Penetration Testing services are delivered by experienced, qualified ethical hackers, and we provide summary reports in an easy to digest format that contain expert advice on how to reduce your organisation's attack surface and close off common vulnerabilities.

Get an attacker's perspective on your current network security so you can fix the vulnerabilities within your infrastructure and applications and help stop ransomware attacks.

The Importance of Penetration Testing

Our Penetration Testing services provide an expert view of your dispersed IT environment, enabling you to understand your vulnerabilities and defend your network no matter where it is located and how it is accessed.

When your IT environment is distributed outside your office, your organisation's exposure to data breach increases.






Our Penetration Testing services enable you to:

- Identify the key vulnerabilities exploited by the most dangerous ransomware groups.
- Understand and reduce the attack surface created by the use of public cloud-based services.
- Test across the breadth of complex environments, providing you with the knowledge you need to maintain effective configurations and cyber security best practices.

- Reduce the threat from reliance on integration with suppliers, partners and customers through APIs, data transfers and applications.
- Illuminate potential software vulnerabilities and ensure critical patches are up-to-date.

Our Penetration Testing Process

We follow a tried and tested methodology when approaching any engagement:

-  **Scoping.** Understand business risks and outcomes to determine the correct assets and testing approach.
-  **Reconnaissance.** Use tools and knowledge to build an initial vulnerability profile.
-  **Assessment.** Assess the susceptibility of any vulnerability discovered.
-  **Reporting.** Contextualised and relevant report detailing the severity of findings and impact if exploited.
-  **Re-test.** Ensure the remedial activities conducted are successful.

What It Does	Why This Matters	What It Means
Expose your weaknesses before real hackers do.	Understanding the risks within your environment ensures you have the correct information to make critical decisions.	Ignorance is not a valid excuse if an organisation is breached. Knowing your vulnerabilities ensures you can plan for the future.
Reveal which areas of security you need to invest in.	Low severity vulnerabilities are often the stepping-stone to a successful breach.	Prioritised reporting that details the actual risk ensures the right effort and resources are focussed on fixing what really matters.
An outsider perspective on your security.	Knowing your infrastructure inside out does not mean that you are fully aware of the security risks that may exist.	Our penetration testers can advise on how best to mitigate threats that exist if normal remediation actions such as patching are not possible.
Simulate a real attack scenario.	Hackers are not bound by the resource and time limitations that businesses are.	Attempting to exploit a vulnerability will demonstrate the effectiveness and possible impact, and tests current controls implemented within the environment.

Our Penetration Testing Credentials



We are the longest running CHECK Accredited Company in the UK. Our highly experienced team of consultants are all CREST accredited.



Our testing team has been at the forefront of penetration testing techniques since 1999.



Our team maintains highly accredited technical certifications including CHECK, CREST, Tigerscheme and Cyber Scheme.



We are not just testers. We have real life experience of running networks and auditing them. Our testing team also have certified ISO 27001 and PCI DSS QSA Audit certifications.



All of our team members have SC clearance.



We have a research team who lab new techniques and hold Pen Test Portal Training quarterly sessions for all clients wishing to learn and understand how to hack.

Partners and Accreditations:



To learn more about our Penetration Testing services, or to book your Penetration Test, contact your Account Manager or visit 6dg.co.uk/pen-testing